IN THE UNITED STATES DISTRICT COURT FOR THE

WESTERN DISTRICT OF OKLAHOMA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
-vs-	)	**No. CR-17-239-M**
	)	
JERRY DRAKE VARNELL,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION FOR HEARING TO DETERMINE ADMISSIBILITY OF GOVERNMENT EXHIBITS AND/OR TESTIMONY

The United States of America, through Robert J. Troester, Acting United States Attorney for the Western District of Oklahoma, by Mark R. Stoneman, Assistant United States Attorney, moves this Court to deny defendant's Motion for Hearing to Determine Admissibility of Government Exhibits and/or Testimony (Doc. 105).

The Defendant's Requested Relief

The defendant asks this Court to "determine the alleged 'screenshots', text messages, and Facebook conversations allegedly made by Mr. Varnell to be inadmissible at trial." (Doc. 105 at 14). This Court should deny these requests.

The Law

The foundational "requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a), *see also United*

States v. Dhinsa, 243 F.3d 635, 658-59 (2d Cir. 2001) (noting Rule 901 "does not erect a particularly high hurdle," and that hurdle may be cleared by "circumstantial evidence") (quoting *United States v. Ortiz*, 966 F.2d 707, 716 (1st Cir. 1992)). Rule 901(a) only requires the government to make a prima facie showing of authenticity or identification "so that a reasonable juror could find in favor of authenticity or identification." *United States v. Chu Kong Yin*, 935 F.2d 990, 996 (9th Cir. 1991); *see also Lexington Ins. Co. v. Western Pennsylvania Hosp.*, 423 F.3d 318, 328-29 (3d Cir. 2005) ("Once a prima facie case is made, the evidence goes to the jury and it is the jury who will ultimately determine the authenticity of the evidence, not the court. The only requirement is that there has been substantial evidence from which they could infer that the document was authentic.") Once the threshold showing has been met to admit the document, any questions concerning the genuineness of the item normally go to the weight of the evidence. *Orr v. Bank of America*, 285 F.3d 764, 773 n. 6 (9th Cir. 2002) ("Once the trial judge determines that there is prima facie evidence of genuineness, the evidence is admitted, and the trier of fact makes its own determination of the evidence's authenticity and weight.")

In the specific context of Facebook messages, the Third Circuit has held,

> [I]t is no less proper to consider a wide range of evidence for the authentication of social media records than it is for more traditional documentary evidence. The authentication of electronically stored information in general requires consideration of the ways in which such data can be manipulated or corrupted…, and the authentication of social media evidence in particular presents some special challenges because of the great ease with which a social media account may be falsified or a legitimate account may be accessed by an imposter… But the authentication rules do not lose their logical and legal force as a result… Depending on the circumstances of the case, a variety of factors

> could help support or diminish the proponent's claims as to the authenticity of a document allegedly derived from a social media website, and the Rules of Evidence provide the courts with the appropriate framework within which to conduct that analysis.

United States v. Browne, 834 F.3d 403, 412 (3rd Cir. 2016), *cert. denied*. 137 S.Ct. 695 (2017) (internal citations omitted) (noting that all the Courts of Appeals that have considered the issue have reached the same conclusion). The defendant in *Browne* challenged the government's authentication at trial of a Facebook account under the name "Billy Button." *Id*. at 408. "To authenticate the messages, the Government was therefore required to introduce enough evidence such that the jury could reasonably find, by a preponderance of the evidence, that Browne and the [other witnesses] had authored the Facebook messages at issue." *Id*. at 410. At trial, witnesses testified about Facebook exchanges they had with the defendant that were consistent with the chat logs introduced by the government, the defendant stated he owned the account and had conversed with the witnesses, the defendant stated he owned the phone containing photos of the witnesses, the defendant confirmed various personal information consistent with personal information interspersed throughout the account conversations, and Facebook provided a certificate attesting to the chat logs' maintenance by its automated systems. *Id*. at 413-415. The Court in *Browne*, found that, "Browne's authentication challenge collapse[d] under the veritable mountain of evidence linking Browne to [the challenged Facebook account] and the incriminating chats." *Id* at 415.

Where the government offers sufficient evidence to authenticate Facebook records as chats the defendant himself participated in, those records are properly admissible as

admissions by a party opponent under Federal Rule of Evidence 801(d)(2)(A). *Browne*, 834 F.3d 403 at 415. Facebook chats in which the defendant did *not* participate in is generally inadmissible hearsay if they are offered to prove the truth of the matter asserted. *Id*. at 416.

Argument

Screenshots

Absent the author or recipient of the screenshots testifying, the government generally agrees that the screenshots would not be admissible to prove the truth of the matters they assert. However, they may be admissible for other purposes, such as to supply context to actions or statements by Mr. Varnell or other witnesses.

Facebook messages

The Facebook records are admissible and relevant. The government anticipates the testimony being that agents obtained the Facebook messages directly from Facebook pursuant to a search warrant. The government anticipates an agent will testify that he communicated with Mr. Varnell via this particular Facebook account. Specific details in the Facebook account show that it covers significant portions of Mr. Varnell's life, including photographs of him and his friends. The government anticipates testimony that during his Mirandized interview, when asked about the undercover agent, Mr. Varnell unlocked his phone, opened the Facebook application and discussed having contact with the undercover agent using Facebook. The government anticipates testimony from an agent who was present during Mr. Varnell's interview that he saw that the account Mr. Varnell accessed on his phone had the same profile picture and username as the records

obtained directly from Facebook. All these factors will be sufficient for a *prima facie* showing to admit the messages in that a reasonable juror could find in favor or their authenticity. *Chu Kong Yin*, 935 F.2d at 996. Mr. Varnell will be free to make arguments to the *jury* as to their weight and credibility. *Orr*, 285 F.3d at 773 n.6.

Claims by the defense that the electronic evidence may have been hacked by a third party should not preclude authentication and should be readily rejected. Questions concerning trustworthiness normally go to the weight of the evidence and not admissibility. As one court noted in dismissing a similar challenge to admit electronic messages"

> [T]his trait is not specific to e-mail evidence. It can be true of any piece of documentary evidence, such as a letter, a contract or an invoice. Indeed, fraud trials frequently center on altered paper documentation, which, through the use of techniques such as photocopies, white-out, or wholesale forgery, easily can be altered. The possibility of alteration does not and cannot be the basis for excluding e-mails, as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents). We live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world. The defendant is free to raise this issue with the jury and put on evidence that e-mails are capable of being altered before they are passed on. Absent specific evidence showing alteration, however, the Court will not exclude any embedded e-mails because of the mere possibility that it can be done."

United States v. Safavian, 435 F.Supp.2d 36, 41 (D.D.C. 2006). For these same reasons, the defendant's argument fails. To the extent statements in the Facebook records can be attributed to Mr. Varnell, they are admissible under Fed. R. Evid. 801(d)(2).

TextLock

The government anticipates offering certain messages made by the defendant to others on social media. The government anticipates testimony and evidence that Mr. Varnell often encrypted these messages so that the messages would appear as garbled nonsense to someone without the decryption key. An encryption key can be neither true nor false in the sense contemplated by the rules of hearsay. Rather, as with conventional door or car keys, either an encryption key works or it does not. The closest analogue for an encryption key might be the combination for a padlock. The three or four digit combination for a padlock is neither true nor false. Either it works letting you see what is contained inside, or it is the wrong combination. Similarly, in the context of TextLock, if the encryption key works, it allows the reader to view the plain text language of what was typed. To the extent that decrypted messages are attributable to Mr. Varnell, they should be admissible. The defendant cites no law that encryption keys are hearsay. For all these reasons, the defendant's argument fails.

Rule 106

The government agrees that admitting context to the defendant's Facebook statements may be appropriate. As noted above, the statements by Mr. Varnell on Facebook or elsewhere are directly admissible against him under Fed. R. Evid. 801(d)(2). The statements of others used in the electronic communications may be admitted not for the truth of the matter, but as non-hearsay to supply context. *See, e.g., United States v. Dupre*, 462 F.3d 131, 136-37 (2d Cir. 2006) (in wire fraud prosecution, e-mails from investors demanding information about defendant's fraudulent scheme were not hearsay

when offered not for truth of the assertion that the scheme was fraudulent, but to provide context for the defendant's message sent in response and to rebut defendant's argument that she did not know scheme was fraudulent; no Confrontation Clause issues arose since the statements were offered for a non-hearsay purpose).

Conclusion

For the reasons stated above, this Court should deny the defendant's Motion to Determine Admissibility.

Respectfully submitted,

ROBERT J. TROESTER
Acting United States Attorney

s/ Mark R. Stoneman
MARK R. STONEMAN
Assistant U.S. Attorney (OBA 22730)
210 Park Avenue, Suite 400
Oklahoma City, Oklahoma 73102
(405) 553-8700 (Office)
(405) 553-8888 (Fax)
Mark.Stoneman@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on April 30, 2018, I electronically transmitted the attached document to the Clerk of Court using the ECF System for filing and transmittal of a Notice of Electronic Filing to the following ECF registrants:

Marna Franklin and Laura Deskin, attorneys for Mr. Varnell

s/ MARK R. STONEMAN
Assistant U.S. Attorney